(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/80596 A1

(51) International Patent Classification[7]: H04Q 11/04, H04J 3/14

(21) International Application Number: PCT/US01/11972

(22) International Filing Date: 11 April 2001 (11.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/547,944 12 April 2000 (12.04.2000) US

(71) Applicant: SYCAMORE NETWORKS, INC. [US/US]; 150 Apollo Drive, Chelmsford, MA 01824-0986 (US).

(72) Inventors: SEARS, William; 41 Farmcrest Avenue, Lexington, MA 02421 (US). ZAHAVI, Joseph; 4 Gardner Lane, Westford, MA 01886 (US). PATEL, Naimish; 32 Monteiro Way, North Andover, MA 01845 (US).

(74) Agents: SCHURGIN, Stanley, M. et al.; Weingarten, Schurgin, Gagnebin & Hayes, LLP, Ten Post Office Square, Boston, MA 02109 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/80596 A1

(54) Title: METHOD FOR PORT CONNECTIVITY DISCOVERY IN TRANSPARENT HIGH BANDWIDTH NETWORKS

(57) Abstract: In a network having a trace capability, a method to track the connectivity of the network uses the trace messages. A network manager creates a list of ports in the network and uses that list to track the connectivity. For each port, the manager first checks whether there is a current connection and if it finds one, the manager enables the transmission of a trace message that identifies the transmitting port. When a trace detected message is received from a port, the network manager updates the list of ports with the connection just reported and disables the trace message that was detected. A port sending a trace message that is not detected is marked as not connected in the list. The method is useful in high bandwidth circuit-based networks, such as optical networks, composed of links of many types and utilizing differing protocols.

TITLE OF THE INVENTION

METHOD FOR PORT CONNECTIVITY DISCOVERY IN TRANSPARENT HIGH BANDWIDTH NETWORKS

CROSS REFERENCE TO RELATED APPLICATIONS

N/A

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

N/A

BACKGROUND OF THE INVENTION

The present invention relates generally to high bandwidth networks and methods used for managing such networks and, more specifically, to optical networks andmethods used for discovering the connectivity of networks.

One traditional way of tracking the the connectivity of communication links in a network has been to record the connectivity manually as the node elements and links are installed and activated. Further updates to the network might not be recorded resulting in the record of the circuit-based network becoming obsolete. As packet-based communications became the primary communications protocol to utilize these networks, computer-controlled management of the packets in network was developed and utilized to track packets. However, similar network management methods were not developed for the circuit-

based underlying structure of the network. Networks that use a protocol that allows for neighbor and connectivity discovery are termed auto-discovering. Packet-based networks, such as TCP/IP and OSI networks use this technique.

In circuit switched networks, however, connections have traditionally been hand-wired. Circuit based protocols were not designed for auto-discovery. While some capability might be designed into the newer optical connection products, the standards for circuit-based networks are currently not sufficiently developed to allow self-discovery of a general circuit-based network. Recently, data bandwidth requirements have increased and the new types of data (digitized video, massive databases, etc) are too fast to be served by packet-based protocols.

High bandwidth networks require entire circuits, the communication connection between two points, to carry data. The need to understand the topology of the layout of circuits is too critical to rely on the unreliable records of the network generated by yesterday's technology. Therefore, there is a need for a methodology of mapping the circuits present in such networks.

BRIEF SUMMARY OF THE INVENTION

A method of determining the connectivity of a circuit-based network uses the information currently available about the network; its nodes, the ports on the nodes, and the type of the links between ports, to support a technique to discover the remaining

connectivity information about the network. A management entity controls the discovery process by enabling transmission of a unique stylized probe message (a TRACE message in the described embodiments) containing transmitter specific information. When a receiver recognizes the message, it reports both the receiver's identity and the transmitter's identity to the management entity. By accumulating this data, the management entity accumulates the connectivity information about the network. Each probe message yields at most one link in the connectivity pattern. The unique stylized probe messages are tailored to the transmission mechanism available at each transmitter. While different types of transmission mechanisms can be used, it is preferable to use the one capable of carrying the most information and disrupting the network least. The management entity that controls the mapping operation can be monolithic, building a map of the entire network in one database, or distributed, allowing maps of subnetworks to reside in multiple nodes hosting management components and one coordinating management resource able to access all the connection information.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The invention will be more fully understood by reference to the following detailed description when considered in conjunction with the accompanying drawings, in which:

Fig. 1 is a schematic of a network according to the invention;

Fig. 2 is a detail of two ports from the network of Figure 1, and their connection as a circuit;

Fig. 3 is a block diagram illustrating participating ports and non-participating ports according to the invention;

Fig. 4 is a state diagram of a port according to the invention;

Fig. 5 is a representative list maintained by a management component in the network of Figure 1, of its ports, their connections and states;

Fig. 6 is a flow diagram of the operation of a management entity discovering the connectivity of the network of Figure 3;

Fig. 7 is a matrix showing the possible input/output characteristics of each side of a port of Figure 2 and the state that corresponds with each; and

Fig. 8 is a state diagram of a managed port according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The methods described herein are applicable to high speed switched networks. Examples from an optical implementation will be used to illustrate such methods.

The network illustrated in Fig. 1 shows two managed circuit based networks 10, 14 that have network-to-network connections traversing a transparent switched network 12. The networks 10 and 14 are connected to respective sets of users via links 18 and 20. The networks 10 and 14 are further connected to the

transparent switched network 12 by network to network connections 16.

The managed circuit switched network 10, includes a management entity (not shown) that tracks the state of the network. The state of the network includes information about physical links interconnecting ports, which ports are being used by a program or user, and which ports are not linked to another port. The transparent switched network 12 is not part of the managed switched network 10, so the management entity in managed switched network 10 doesn't know the state of the connections in the transparent switched network 12. If the elements of Fig. 1 are part of a larger managed network, a coordinating management resource (not shown) needs to know the connections that pass through the transparent switched network 12. However, the management entity in the managed switched network 10 generally does not know the connectivity within the transparent network 12, nor where connections 16 terminate in the transparent network 12. Additionally, in transparent networks it is not possible to modify the traffic stream in order to determine connectivity.

Figure 2 shows a detail of two interconnected ports in the network. Bi-directional ports are represented by 30 and 32. The bi-directional port 30 incorporates two sides, a transmitter 38 transmitting information from A to B, and a receiver 34 receiving information transmitted from B to A. The link 31 may consist of one fiber carrying signals in both directions, or a pair of fibers, each carrying one unidirectional signal.

A receiver such as 34 is generally always active. It is monitoring its input. The receiver 34 either receives nothing or it receives information in a form it can interpret. Thus, a receiver connected to a management entity can inform the management entity whether it is connected to an active transmitter. If the transmitter 36 sends a unique message, called a TRACE message, then receiver 34 can detect this message and report it to the management entity.

The mechanism for carrying a TRACE message can be other than a normal information carrying mechanism; it could be a unique frequency, a variation in voltage, or some other pre-arranged mechanism. The TRACE message also carries unique information such as an identifying address which can be passed on to the management entity allowing the management entity to infer the existence of a circuit between the reporting receiver 34 and the transmitter 36 sending the unique message. The transmitter 36, on the other hand, is passive. It merely transmits a signal presented to it irrespective of the presence of a receiver. The transmitter can send a unique signal, but cannot detect whether it is received nor identify the receiver.

Fig. 3 illustrates the communications between ports and management components including coordinating management resources. A first set of ports 63, 64, and 65 report to one management component 60. A second set of ports 66, 67,and 68 report to another management component 58. Because of the connections between ports, management component 60 learns of ports 67 and 68, and management component 58 learns of ports 63 and 64. In

addition, management component 60, due to its connection with port 65, learns of port 69, which does not report to any management component. Ports 54 and 56 are connected to each other, but do not participate in the managed network because neither one of them reports to a management entity. The coordinating management component 62 may maintain an overall database of ports in the entire managed network and/or may facilitate the transfer of information between all management resources including ones not shown.

The management entity tracks the status of each port using a sequence of states as illustrated in Fig. 4. A port can be either connected to another port or disconnected. Line 71 separates the port state diagram into a connected side containing state 80 and disconnected side containing states 70 and 74. A port starts in state NOT-CONNECTED 70 meaning that the port can report to the management entity but is not transmitting to nor receiving from any other port. A management command 72 moves the port into the TRACING state 74 meaning that the transmitter side of the port is sending a unique message (the TRACE message) that, if received and reported to the management entity by a managed receiver, allows the management entity to infer a link between the two ports. The port remains in the TRACING state 74 until the port's TRACE message has been received by a receiver whereupon a management command 78 moves the port into the CONNECTED state 80. When the port is in CONNECTED state 80, it is available for use by communications applications programs. If the port's TRACE message is not reported as received within a

predetermined time, the management entity sends a command 75 that causes the port to transition from the TRACING state 74 to the NOT-CONNECTED state 70. When a port has entered the CONNECTED state 80, it remains in the CONNECTED state 80 until the connection to its counterpart is lost. When the management entity is informed of the lost connection, it sends a command 82 that moves the port to the NOT-CONNECTED state 70.

The management entity tracks port connectivity and tracing activity using a port list such as illustrated in Fig. 5, which shows a port list in the Coordinating Management Component 62 of Figure 3. Fig. 5a illustrates an initial state of the list, for example upon power-up of the management unit or power-up of the entire network. The management entity knows of a number of ports by their ID, and for some of those ports knows the physical layer protocol or physical connection type. For instance in Fig. 5a, Port 63 is known to use the SONET protocol and Port 66 to use Ethernet. Techniques to determine the type of connection are well known in the art. It is assumed that appropriate techniques are used to determine the connection types for the remaining ports, and these values are then entered in the port list as shown in Fig 5b.

In an alternate embodiment, if the management entity has a record of the interconnection of ports in the network from some source, such as manual records, the management entity could provisionally fill in the "Connected to" column of the list. These initial connections would be subject to verification by the TRACE mechanism, but would provide connection information for

unmanaged ports. The verification would update the manual records for broken links, unrecorded upgrades or faulty equipment.

In an embodiment of the invention, initialization of the management port list of Fig. 5 and the network is tracked as shown in Fig. 5a through 5d and takes the form of the steps in the flowchart of Fig. 6. The management entity first establishes a reporting relationship with each port that it will be managing and receives status from each port, step 100. At the end of this operation, the port list has been updated as shown in Fig. 5b, in which ports 63 and 68 are shown as connected to ports 68 and 63 respectively and port 66 is shown as connected, but to an unknown port. Port 66 could be, for instance, connected to a user device.

Connectivity is then discovered using a path tracing technique that employs TRACE messages as mentioned above. A TRACE message is a unique message, distinguishable from a regular transmission, which carries information that can be interpreted by some receivers and reported back to a management entity. The report from the receiver allows the management entity to discover the link between the receiver and the transmitter that is sending the TRACE message.

As previously mentioned, the TRACE message may be carried over a link using any of a variety of TRACE mechanisms. The TRACE mechanisms may be stored in a database or a list and the "type of connection" entry in the port list of Fig. 5 provides a pointer for the management entity as to what type of TRACE mechanism to use. For example, a SONET link TRACE message could be

sent using a pattern in the J0 (section trace) bytes. A Gigabit Ethernet link TRACE message could be sent using a standard packet or could use unused codewords of the 8B/10B code. For a transparent link capable of low frequency modulation and detection a TRACE message could be sent by varying the voltage of the signal. A TCP/IP or OSI link TRACE message could be sent using the self discovery capabilities built into the protocol. For a link where the signal can be turned on and off, and where the presence of a signal can be detected, a TRACE message could be sent by turning power on and off in a Morse Code like pattern. For a link capable of handling a subcarrier, such as one using some analog component before signal detection, a TRACE message could be sent by placing signals on a sub carrier. Finally, for a link where information is encoded into forward error correction frames, a TRACE message could be sent using Forward Error Correction Frames. This technique can be extended to any link where information is encoded into frames, and at least some of the bits are available when the frames are not carrying traffic. For some types of connection, multiple TRACE mechanisms could be possible, with the success of a particular mechanism dependent on the higher level protocols being used on the link. As an alternate embodiment, multiple parallel TRACE mechanisms may be initiated at one port, with the mechanism that successfully detects the connection being utilized for further TRACEs. As standards are developed in the optical networking realm, the management entity will be able to use the least intrusive and most informative standard supported by the link.

The TRACE message includes a TRACE signature to distinguish the TRACE message from another transmission, an identification of the transmitter port to allow the management entity to identify both ends of the link, and an identification of the management entity that needs to know the transmitter and receiver that define the link. The TRACE signature can be an unlikely constant value or some function of the rest of the data in the message. A type of checksum is one such function. The checksum can be further encoded by adding in a unique value to a message-computed checksum. A separate management component, such as the receiver's management component, may receive the initial TRACE report from the receiver, but that information will be passed through the distributed management to the identified management entity.

Referring to the flow diagram of Fig. 6, after the first contact with the ports is accomplished in step 100, the management entity directs a set of transmitters to send unique TRACE messages into the network, step 104. In a preferred embodiment, groups of transmitters source TRACE messages simultaneously, although for an initial setup situation, all disconnected ports could TRACE simultaneously. The management port list is further updated to the state of Fig. 5c, where port 65 is shown as TRACING. The management entity waits a predefined time for reports from receivers, step 106. Each time a report (referred to as a TRACE detected message) is received, the management port list is updated and the TRACE message(s) for that link are terminated, step 108. One report may cause termination of two TRACE messages, the

TRACE message that caused the report by the receiving port and any TRACE message currently being sent by the transmitting side of the receiving port.

In a preferred embodiment, as a failsafe mechanism in case the management entity does not respond in a timely manner, the receiver of a port that has recognized a TRACE message terminates any TRACE message being sent by its own transmitter.

Once the predefined time has elapsed, an additional set of transmitters is directed to send TRACE messages, step 104 as shown in Fig. 5d, until all initially NOT-CONNECTED transmitters known to the management entity have been in the TRACING state. Once all disconnected ports have undergone a TRACE, the linked ports are freed to communicate in Step 110 by making the ports available to a communications program. Alternatively, linked ports are freed to communicate as soon as the management entity is sure that any TRACING of the line has been terminated. The management entity continues TRACING disconnected ports, step 112, according to a predetermined algorithm such as a round robin, while managing other aspects of the network. When all ports known to the management entity are connected, the management port list will look like Fig. 5e.

The management entity can serve functions other than the TRACING function. For example, for Ethernet links, the management entity can supply a port with its counterpart's IP address at the time the physical address of the link is reported.

The management entity presumes that links remain connected unless a communications program reports a

disconnect. When a disconnect between two ports is reported, the management port list is updated to show that the ports are now NOT-CONNECTED, and a TRACE of that link is scheduled according to the predetermined algorithm.

An alternate way of viewing the state of a port is by the actions being performed by the two sides of the port as shown in Fig. 7. If the receiver is receiving data as shown in column 2 of Fig. 7, the port is in the CONNECTED state 80 regardless of what the transmitter is doing. The transmitter is not allowed to be sending a TRACE when its receiver is receiving. Similarly, if the receiver is receiving a valid carrier as shown in column 4 of Fig. 7, the port is in the CONNECTED state 80 and the transmitter is not allowed send a TRACE message. If the receiver has nothing on its input as shown in column 5 of Fig. 7, the port is disconnected. When the transmitter is TRACING while the receiver has nothing on its input, the port is in the TRACING state 74. If the transmitter is idle, the port is in the NOT-CONNECTED state 70. If the transmitter is sending data while the receiver has nothing on its input, the port is disconnected, but there is an error condition - likely a false positive on the transmitter. Similarly, if the receiver is receiving something other than data or a valid carrier as shown in column 3 of Fig. 7, the port is disconnected and can be in either the NOT-CONNECTED state 70 or TRACING state 74.

The method of using TRACE messages to discover connectivity can be extended to monitoring an active network. In this mode, the management entity uses an

algorithm to choose which circuits to monitor. This algorithm can be based on a variety of information sources available to the management entity, such as user configuration, traffic type, incidence of false positive connections, and length of connection. The management port list is updated as shown in Figure 5f to indicate that a port is being MONITORED. The TRACE message used for monitoring is a low-information-rate trace sent using a mechanism that is known not to be disruptive to the particular circuit. For example, information could be sent via the section trace byte in a SONET message by occasionally changing the byte.

The sequence of states employed for active monitoring is illustrated in the state diagram of Fig. 8. Line 118 separates the port state diagram into a connected side containing states 80, 136and 154 and a disconnected side containing states 70 and 74. The disconnected side of the Figure 8 is the same as illustrated in Figure 4, while the connected side adds the MONITORED state 136 and the DISRUPTED state 154. When a connection to a port in the CONNECTED state 80 is lost, a management command 82 places the port in the NOT-CONNECTED state 70. If the CONNECTED port is to be monitored, a management command 134 puts the port into the MONITORED state 136 where monitoring traces are sent to the port by its counterpart. The port normally stays in the MONITORED state 136 until returned to the CONNECTED state 80 by a management command 140. If a disruption in the monitoring is detected, the port being MONITORED reports this to the management entity which issues a command 152 placing the port in the DISRUPTED

state 154. If the disruption is cleared quickly enough, a later management command 150 will return the port to the MONITORED state 136. If the disruption is not cleared quickly, a management command 144 places the port in the NOT-CONNECTED state 70.

Preferred embodiments of the invention having been described, it will be apparent to those skilled in the art that other embodiments incorporating these concepts may be used. Accordingly, it is submitted that the invention should not be limited by the described embodiments but rather should only be limited by the spirit and scope of the appended claims.

CLAIMS

1. A method of determining connectivity in circuit-based networks made up of a plurality of nodes having a plurality of ports connected by links, each port having a transmit side and a receive side, the method comprising:

for a first port that is not receiving user data from any other port, enabling a trace message from the transmit side of said first port;

monitoring for a trace detected message from a second port; and

on receipt of said trace detected message, recording the existence of a link between said first port and said second port.

2. The method of claim 1 further comprising disabling said trace message from said transmit side of said first port upon receiving said trace detected message from said second port.

3. The method of claim 2 further comprising allowing user communications between said first port and said second port after said trace message is disabled.

4. The method of claim 1 wherein said circuit-based network is an optical circuit-based network.

5. The method of claim 1 wherein said circuit-based network is a circuit-based transparent network.

6. The method of claim 1 wherein said method is executed by a management entity in said network.

7. The method of claim 6 wherein said management entity is a distributed manager having a plurality of management resources, each management resource having a port/link table for ports of network nodes associated with said management resource.

8. The method of claim 7 wherein said second port reports said trace detected message to said distributed manager via said management resource associated with said second port.

9. The method of claim 6 wherein said management entity maintains a port/link table for ports of network nodes and wherein each port/link table entry has associated with it a type of connection

10. The method of claim 9 wherein said management entity has a database of different trace mechanisms, each mechanism to be selected based on said type of connection.

11. The method of claim 10 wherein said trace message is encoded by powering a carrier signal on and off at a low rate.

12. The method of claim 10 wherein said trace message is encoded as a signal on a sub-carrier frequency that is compatible with said connection on said link.

13. The method of claim 10 wherein said trace message is encoded as a special packet type.

14. The method of claim 10 wherein said trace message is encoded in forward error correction frames at system startup.

15. The method of claim 1 wherein said trace message includes a management address, a trace signature and a port identifier.

16. The method of claim 1 wherein said second port disables a trace message from said transmit side of said second port upon receiving said trace message.

17. A method to track the connectivity of a network comprising the steps of:

creating a list of ports in said network;

for each port, determining whether said port is connected to another port and if connected, recording the connection between said two ports in said list;

for each unconnected port, enabling the sending of a trace message from said port;

receiving trace detected messages from ports in said network and recording in said list a connection between the port detecting said trace message and the port sending said trace message;

disabling the trace message for ports whose trace has been received and allowing user communication on the connections for such ports; and

terminating trace operations for ports whose trace has not been received after a first predetermined time.

18. The method of claim 17 further comprising reinitiating a trace after a second predetermined time.

19. The method of claim 17 further comprising;

polling said known ports to determine if a trace message has been received, and updating said list based on the response.

20. A method of operation of a port having a transmitter and a receiver in an optical network comprising:

at power-up, initiating a first trace message from said transmitter and monitoring for receipt of a second trace message at said receiver;

on detection of said second trace message, sending a first message to a management component; and

on detection of a communication not incorporating said second trace message, discontinuing said first trace message and sending a second message to said management component.

21. A method of tracing the linkage of a port adapted to send serial communications in a completely transparent optical network comprising:

driving a transmitter of said port by modulating a power level in a coded manner to send a trace message;

detecting said modulation of the power level at a receiver of a different port; and

reporting said detection of said trace message to a management component.

22. A method of monitoring an optical network composed of a plurality of types of connections having a trace capability comprising;

determining that connectivity is established on a link;

sending a low-information rate trace utilizing a mechanism known not to be disruptive on the link;

receiving a trace detected message within a predetermined time and comparing information in said trace detected message with said established connectivity; and

if no trace detected message is received within the predetermined time, regarding the link as disconnected.

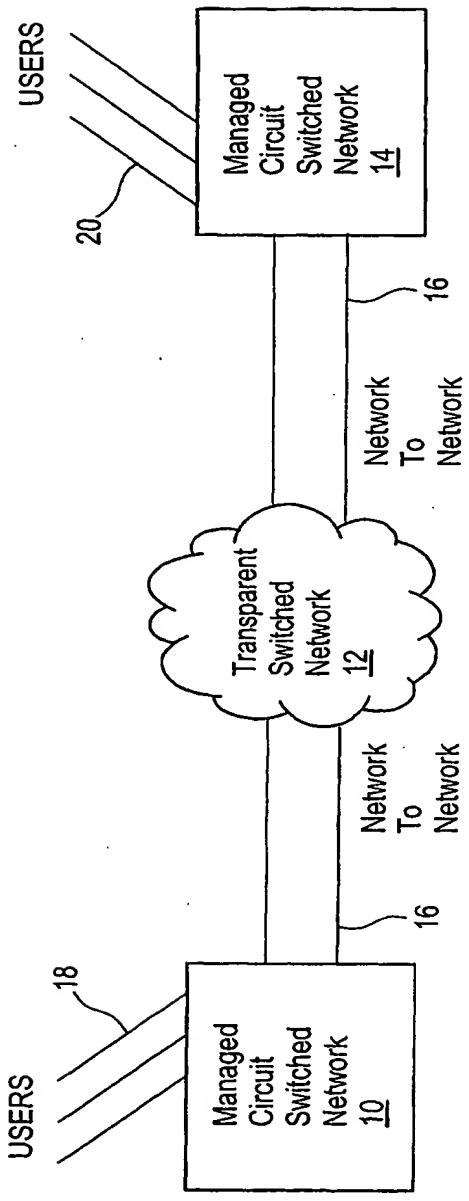
USERS
20
Managed Circuit Switched Network 14
16
Network To Network
Transparent Switched Network 12
Network To Network
16
18
USERS
Managed Circuit Switched Network 10

FIG. 1

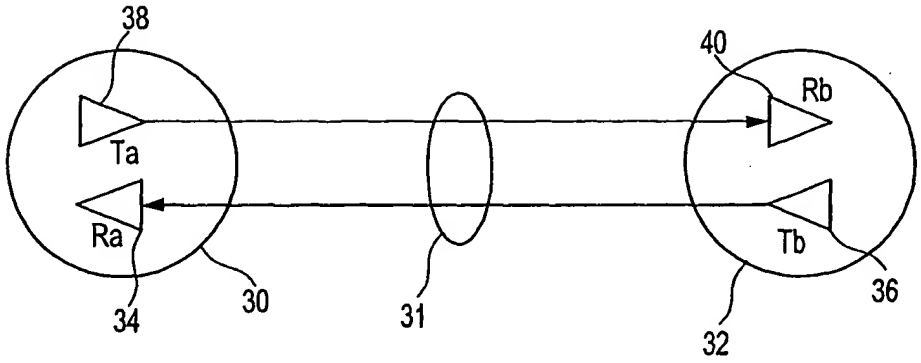
38
40
Rb
Ta
Ra
Tb
34
30
31
32
36

FIG. 2

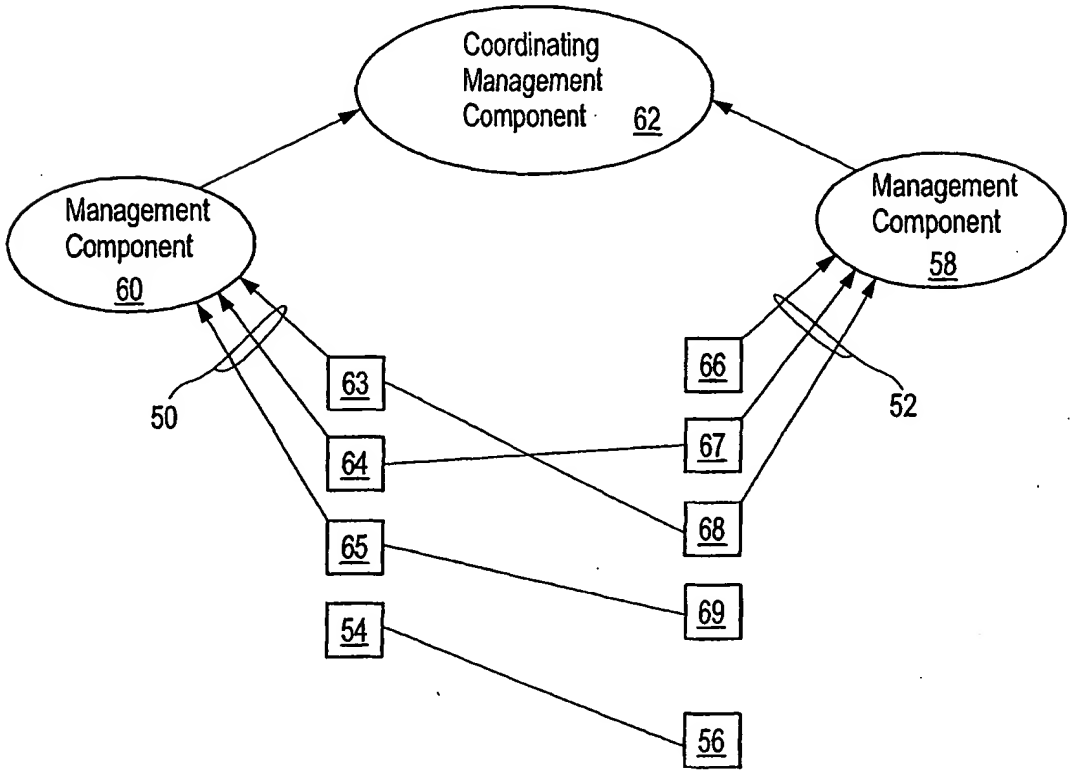
Coordinating
Management
Component
62
Management
Component
60
Management
Component
58
50
52
63
64
65
54
66
67
68
69
56

FIG. 3

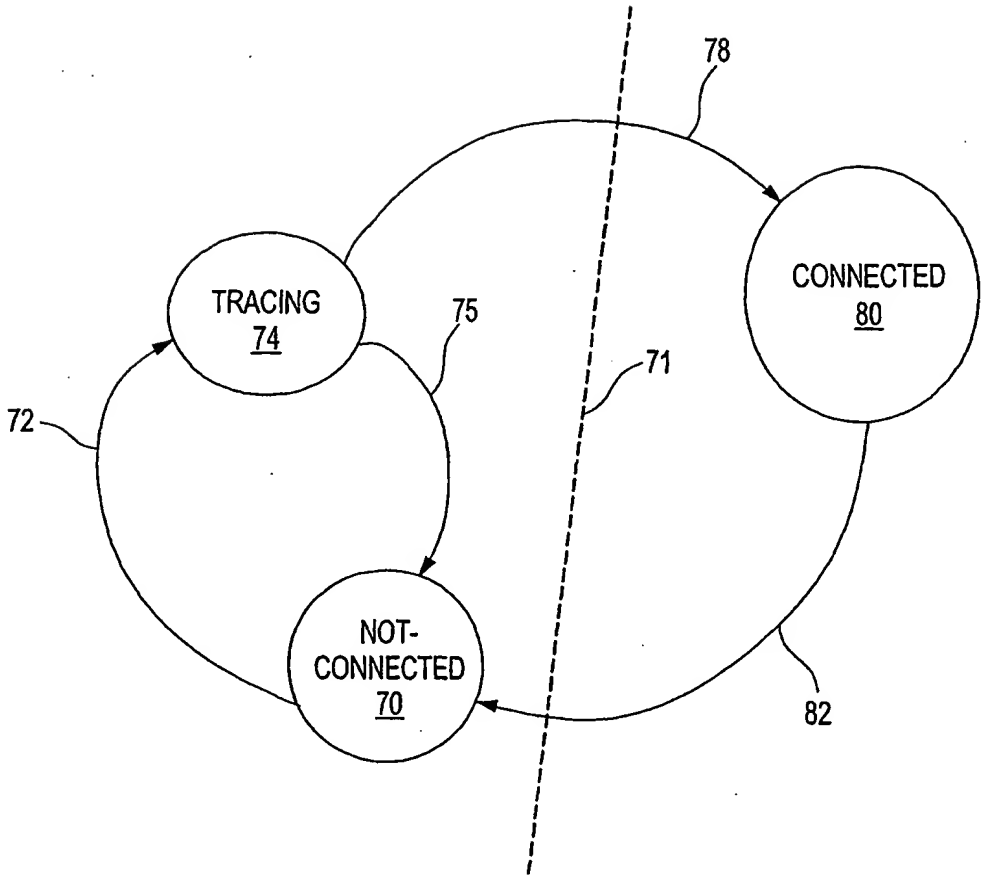

FIG. 4

Port ID	Connected to	Type of Connection	State
63		SONET	
64			
65			
66		Ethernet	
67			
68			

FIG. 5a

Port ID	Connected to	Type of Connection	State
63	68	SONET	CONNECTED
64		ATM	NOT-CONNECTED
65		FDDI	NOT-CONNECTED
66		Ethernet	CONNECTED
67		ATM	NOT-CONNECTED
68	63	SONET	CONNECTED

FIG. 5b

Port ID	Connected to	Type of Connection	State
63	68	SONET	CONNECTED
64		ATM	NOT-CONNECTED
65		FDDI	TRACING
66		Ethernet	CONNECTED
67		ATM	NOT-CONNECTED
68	63	SONET	CONNECTED

FIG. 5c

Port ID	Connected to	Type of Connection	State
63	68	SONET	CONNECTED
64		ATM	TRACING
65	69	FDDI	CONNECTED
66		Ethernet	CONNECTED
67		ATM	NOT-CONNECTED
68	63	SONET	CONNECTED

FIG. 5d

Port ID	Connected to	Type of Connection	State
63	68	SONET	CONNECTED
64	67	ATM	CONNECTED
65	69	FDDI	CONNECTED
66		Ethernet	CONNECTED
67	64	ATM	CONNECTED
68	63	SONET	CONNECTED

FIG. 5e

Port ID	Connected to	Type of Connection	State
63	68	SONET	MONITORED
64	67	ATM	CONNECTED
65	69	FDDI	CONNECTED
66		Ethernet	CONNECTED
67	64	ATM	CONNECTED
68	63	SONET	CONNECTED

FIG. 5f

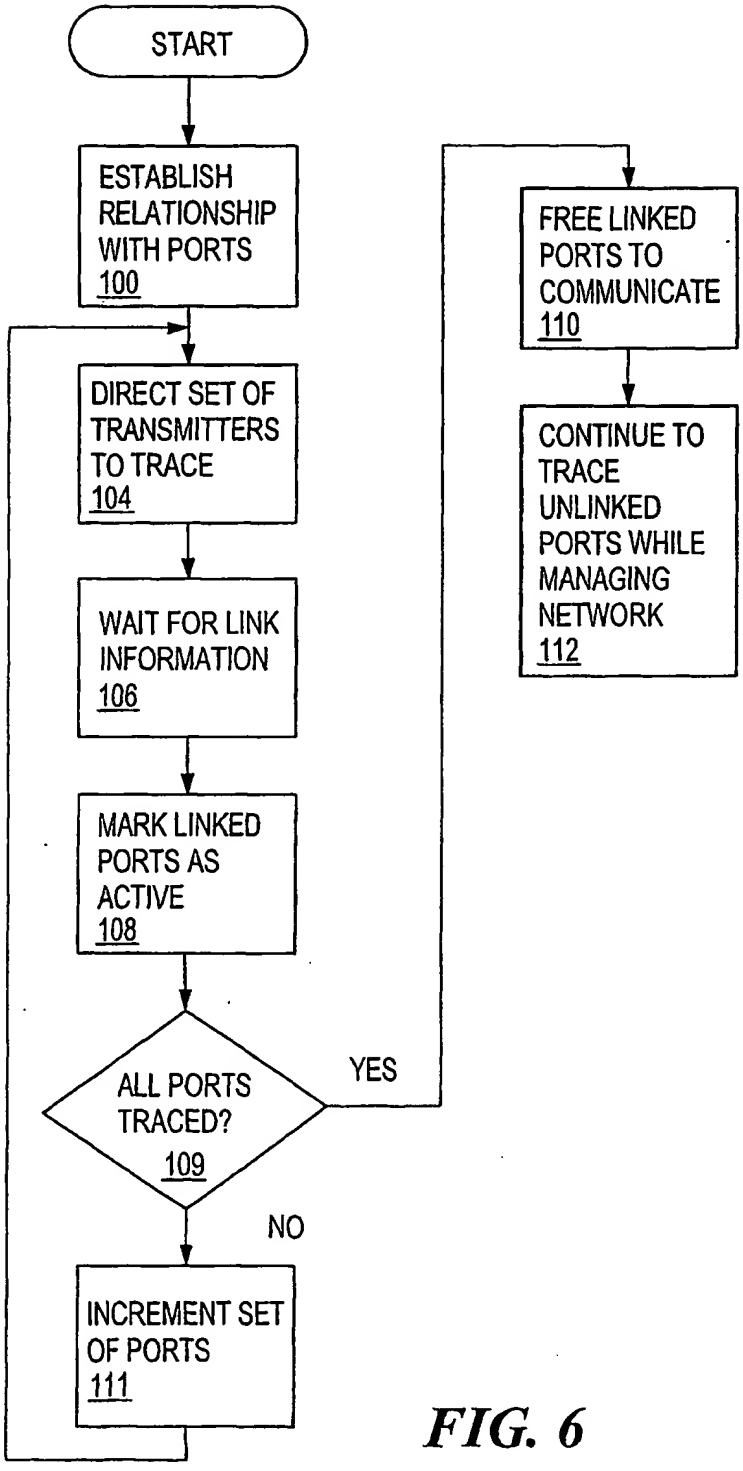
START
ESTABLISH RELATIONSHIP WITH PORTS 100
DIRECT SET OF TRANSMITTERS TO TRACE 104
WAIT FOR LINK INFORMATION 106
MARK LINKED PORTS AS ACTIVE 108
ALL PORTS TRACED? 109
YES
NO
INCREMENT SET OF PORTS 111
FREE LINKED PORTS TO COMMUNICATE 110
CONTINUE TO TRACE UNLINKED PORTS WHILE MANAGING NETWORK 112

FIG. 6

RCVR / XMITTER	RECEIVING DATA	RECEIVING BUT NOT DATA	RECEIVING CARRIER	NOT RECEIVING
TRACE	N/A - CONNECTED	TRACING	N/A - CONNECTED	TRACING
IDLE	CONNECTED	NOT-CONNECTED	CONNECTED	NOT-CONNECTED
SENDING DATA	CONNECTED	ERROR CONDITION	CONNECTED	ERROR CONDITION

FIG. 7

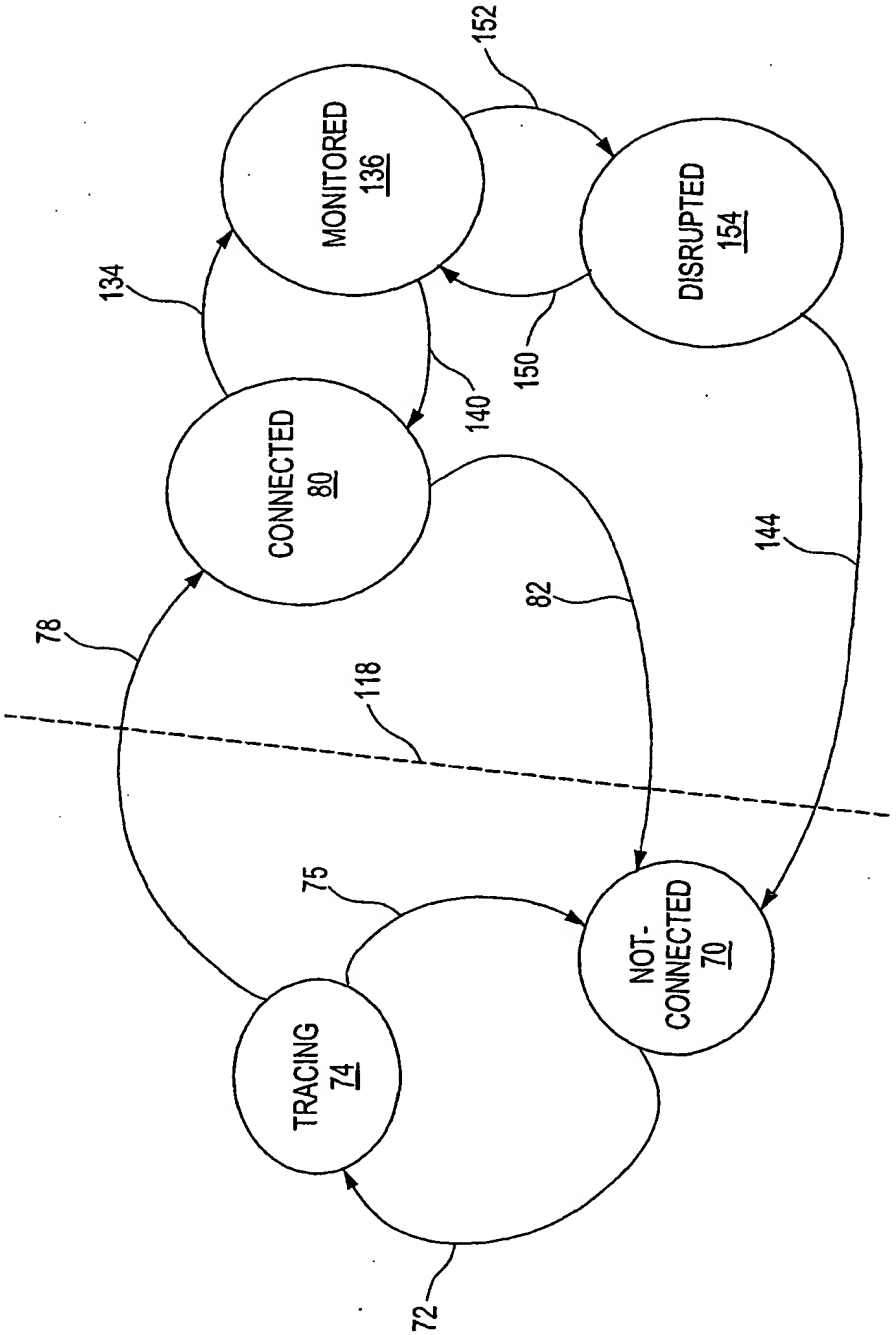
MONITORED
136
DISRUPTED
154
CONNECTED
80
TRACING
74
NOT-
CONNECTED
70
152
134
150
140
144
82
78
118
75
72

FIG. 8

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q11/04 H04J3/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 50986 A (ALCATEL USA SOURCING LP) 7 October 1999 (1999-10-07) page 16, line 5 -page 17, line 10 ---	1,17, 20-22
A	WEI J Y ET AL: "NETWORK CONTROL AND MANAGEMENT OF A RECONFIGURABLE WDM NETWORK" MILCOM 1996 CONFERENCE PROCEEDINGS. CONFERENCE. MCLEAN, VA, OCT. 21 - 24, 1996, ANNUAL MILITARY COMMUNICATIONS CONFERENCE, NEW YORK, IEEE, US, vol. 2 15TH, 22 October 1996 (1996-10-22), pages 581-586, XP000697343 ISBN: 0-7803-3683-6 paragraph '03.1! --- -/--	1-22

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 September 2001	09/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Staessen, B

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SONE T ET AL: "A FLOATING TRACK METHOD FOR COMPLETE ROUTING" ELECTRONICS & COMMUNICATIONS IN JAPAN, PART II - ELECTRONICS, SCRIPTA TECHNICA. NEW YORK, US, vol. 69, no. 8, 1986, pages 20-29, XP000716216 ISSN: 8756-663X abstract	1-22
A	WO 99 57841 A (LIBIT SIGNAL PROCESSING LTD ;SHALVI OFIR (IL); SEGAL MORDECHAI (IL) 11 November 1999 (1999-11-11) page 7, line 5 - line 12	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

I tional Application No
PCT/US 01/11972

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9950986 A	07-10-1999	EP 1072115 A1	31-01-2001
		WO 9950986 A1	07-10-1999
WO 9957841 A	11-11-1999	AU 3531699 A	23-11-1999
		EP 1075744 A1	14-02-2001
		WO 9957841 A1	11-11-1999